



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

AF/3621
#118
10-15-03
mel

In re Patent Application of:

)Attorney Docket No.: F-189

Robert A. Cordery et al.

)Group Art Unit: 3621

Serial No.: 09/650,174

)Examiner: J. Hayes

Filed: August 29, 2000

)Date: October 3, 2003

RECEIVED

OCT 09 2003

GROUP 3621

Confirmation No.: 9744

Title: SECURE USER CERTIFICATION FOR ELECTRONIC COMMERCE EMPLOYING
VALUE METERING SYSTEM

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

10/08/2003 DTESSEM1 00000055 161885 09650174

01 FC:1402 330.00 DA

APPELLANT'S BRIEF ON APPEAL

Sir:

This is an appeal pursuant to 35 U.S.C. § 134 and 37 C.F.R. §§ 1.191 et seq. from the final rejection of claims 35 and 36 of the above-identified application mailed May 8, 2003. The fee for submitting this Brief is \$330.00 (37 C.F.R. § 1.17(c)). Please charge Deposit Account No. **16-1885** in the amount of \$330.00 to cover these fees. The Commissioner is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. **16-1885**. The Notice of Appeal was received by the U.S. Patent and Trademark Office on August 11, 2003. Enclosed with this original are two copies of this brief.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on October 3, 2003
Date of Deposit

Signature

Brian A. Lemm
Name of Registered Rep.

October 3, 2003
Date

I. Real Party in Interest

The real party in interest in this appeal is Pitney Bowes Inc., a Delaware corporation, the assignee of this application.

II. Related Appeals and Interferences

The appeal in the following related cases may have a bearing on the Board's decision in this appeal:

U.S. Application Serial No. 09/650,177, filed August 29, 2000; and

U.S. Application Serial No 09/650,176, filed August 29, 2000.

III. Status of Claims

Claims 35 and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer (U.S. Patent No. 4,868,877) in view of Kuzma (U.S. Patent No. 5,771,289).

IV. Status of Amendments

There are no amendments to the claims filed subsequently to the final rejection of May 8, 2003. Therefore, the claims as set forth in Appendix A to this brief are those as set forth before the final rejection.

V. Summary of Invention

Appellant's invention relates to a secure user certification system for electronic commerce that provides an accounting system for services provided. In electronic commerce,

various parties conduct activities without face to face contact. As such, it is desirable for each party to any transaction to be able to determine and verify the authenticity of the other party to the transaction, as well as ensure sufficient security for any commerce conducted electronically. Such security services could include, for example, message integrity, message authentication, message confidentiality, and message non-repudiation. In an electronic commerce environment these security services are achieved by cryptographic techniques such as digital signature, hash codes, encryption algorithms, and the like. To effectively implement the above, a party to an electronic commerce transaction requires access to a secure cryptographic device capable of securely implementing these cryptographic techniques. According to the present invention, a certificate meter provides certificate management services including use of cryptographically secured certificates. Payment for the processing and issuing, by the certificate authority, of the electronic certificates can be made using funds stored in the meter. Thus, the present invention provides a party to an electronic commerce transaction access to a secure cryptographic device, i.e., a certificate meter, associated with a certificate authority, while providing the certificate authority with a convenient payment system to allow the certificate authority to get paid for processing and issuing of the electronic certificates.

Additional features of the invention are discussed below in the Argument section of this Brief.

VI. Issues

A. Whether the subject matter defined in claims 35 and 36 would have been obvious over Fischer in view of Kuzma.

VII. Grouping of Claims

Claims 35 and 36 are grouped in the following groups:

Group I - Claims 35 and 36.

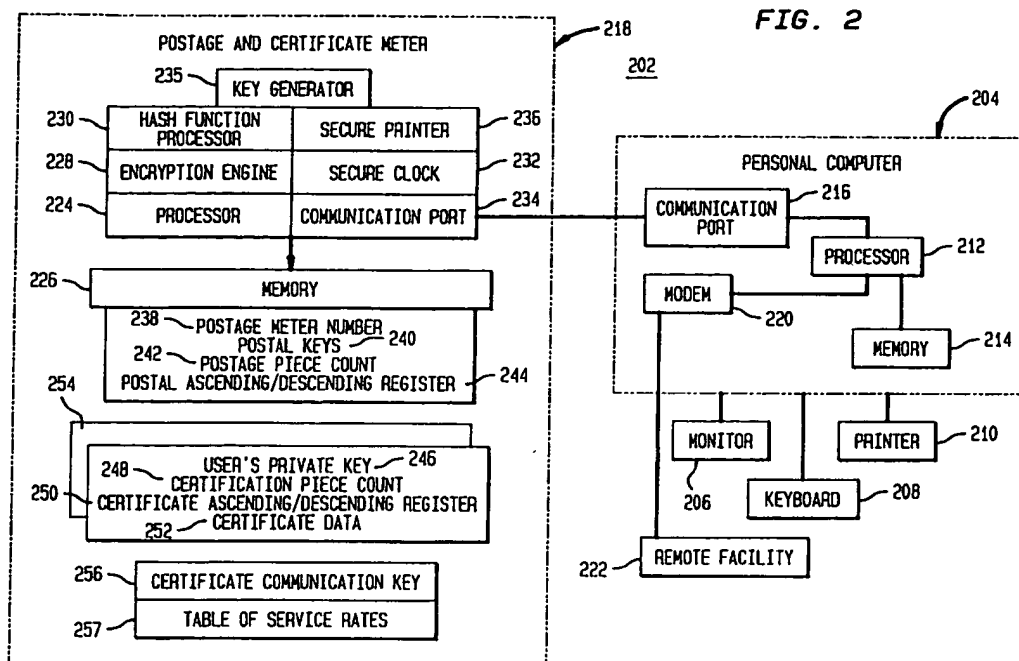
All claims in Group I stand or fall together.

VIII. Argument

As Appellant discusses in detail below, the final rejection of claims 35 and 36 is devoid of any factual or legal premise that supports the position of unpatentability. It is respectfully submitted that the rejection does not even meet the threshold burden of presenting a prima facie case of unpatentability. For this reason alone, Appellant is entitled to grant of a patent. In re Oetiker, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992).

A. The subject matter defined by claim 35 would not have been obvious over Fischer in view of Kuzma.

Fig. 2 of the present specification, reproduced below, illustrates a value metering system in which the processing of cryptographic certificates, including validation of a certificate, according to the present invention is performed. The value and certificate metering system shown generally at 202 includes a personal computer 204 having a monitor 206, a keyboard 208, and is connected to a printer 210. The personal computer 204 additionally includes a processing subsystem 212 having an associated memory 214. The processor is connected to a communications port 216 for communication with a secure postage and certificate meter subsystem 218 and a modem 220 for communicating with a remote facility 222. It should be recognized that many variations in the organization and structure of the personal computer 204 as well as the postage metering and certificate metering subsystem 218 can be implemented. As an example, the communications from the modem to the remote facility can be by way of hardwire or can be by way of radio frequency communications or other communications. The postage and certificate metering subsystem take many forms, for example it may be a secure vault type system, or a secure smart card system.

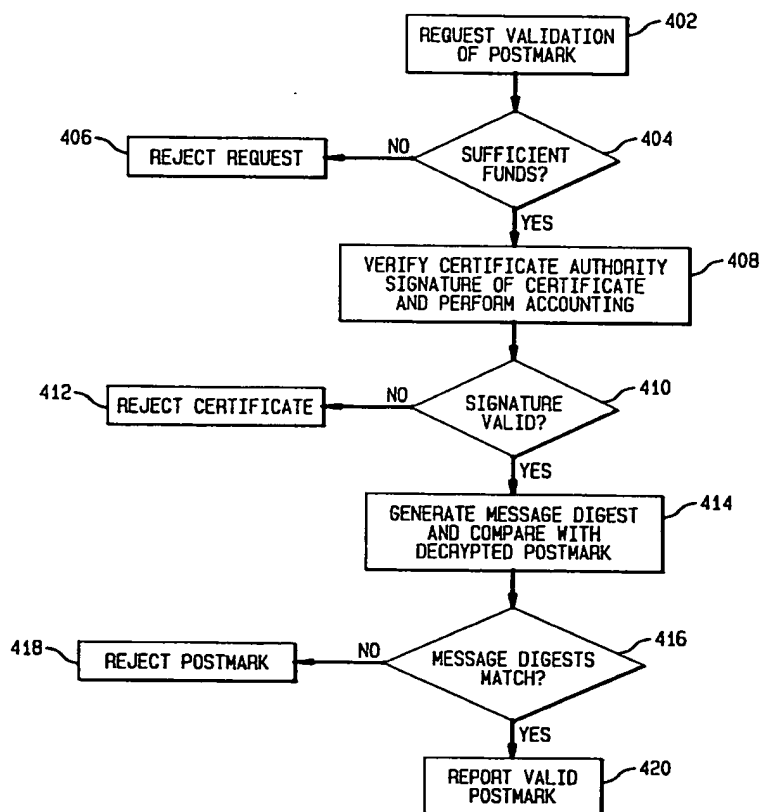


The postage and certificate meter subsystem 218 includes a processor 224 coupled to a memory 226. The processor has associated with it an encryption engine 228, a hash function processor 230, a secure clock 232 and a communications port 234. A key generator 235 is also provided for generating keys for use by the postage and certificate meter. If desired, either a secure printer or a non-secure printer may be connected to the postage and certificate meter subsystem 218, if a printing capability is desired. In Fig. 2, a secure printer is shown at 236. The memory 226 may have stored within it different data as well as the operating program for the postage and certificate meter subsystem 218. The data shown as stored in the memory include the postage meter serial number 238, postal keys 240, postage piece count 242, postage ascending/descending register 244. Additionally stored within the postage and certificate meter 218 memory 226 are user's private key 246, certificate piece count 248, and certificate ascending/descending register 250. This register may be combined with the postage ascending/descending register. Other certificate data shown generally at 252 may also be stored in the memory as well as a certificate communications key 256. A Table of Services Rates is provided at 257. This table includes the rates for the various services that may be obtained when

processing a cryptographic certificate and/or when processing a digital token. As is shown by memory area 254, more than one certificate may be stored in the memory 226. (Specification, page 10, line 10 to page 13, line 11).

Fig. 4 of the present specification, reproduced below, depicts the validation of a cryptographic postmark as performed by the value and certificate metering system illustrated in Fig. 2. A cryptographic postmark is a data file that may contain a message digest, date, time and other data that may be required to provide security services. It should be noted the term "postmark" as used in the present application is not the same as a conventional postmark for printing on a physical mailpiece. The term postmark as used in the present application denotes an electronic certificate for a digital message, i.e., a cryptographic certificate adapted to provide security functionality for the digital message.

FIG. 4



As illustrated in Fig. 4, a request for validation of the postmark is initiated at 402. A determination is made at 404 if sufficient funds are available within the postage and certificate meter subsystem 218. The funds may be stored in the descending certificate register 250 in memory 226, the descending postal register 244 of memory 226, or other registers within the subsystem 218 containing an indication of available funds of the user or party paying for the postmark. (Specification, Page 14, lines 7-11). If sufficient funds are not available the request is rejected at 406. If sufficient funds are available the requester utilizes the certificate authority's public key to verify the signature of the certificate at 408 and accounts for it. If the signature is determined not to be valid at 410, the certificate is rejected at 412. If the signature is determined to be valid at 410, a message digest is generated and compared with the decrypted postmark at 414. A determination is made at 416 if the generated message digest and the message digest in the decrypted postmark match. If they do not match the postmark is rejected at 418. If, on the other hand, they do match, the postmark is reported as valid at 420. (Specification, page 16, lines 7-21).

Thus, the certificate meter of the present invention is a secure cryptographic device with secret information that allows secure communication with a certificate authority such as a post office or other trusted third party and the capability to use, manage and execute various security services. The certificate meter of the present invention includes metering and accounting capability that allows convenient low cost payment of charges per use of a certificate.

In view of the above, claim 35 is directed to a method for validating a signed digital message. Specifically, claim 35 recites:

A method for validating a signed digital message, comprising the steps of:

providing a register having funds stored therein;

receiving a signed digital message from a sender;

determining if sufficient funds are present in the register for validating the message;

deducting funds from the register for validating the message; and

validating the signed digital message using a public key of the sender.

Fischer, in contrast, is directed to a public key cryptographic system with enhanced digital signature certification that authenticates the identity of the public key holder. Specifically, in Fischer, a trusted authority creates a digital message, which contains the claimant's public key and the name of the claimant, and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often referred to as a certificate, is sent along with the use of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key. (Col. 3, lines 21-34). While Fischer discloses the use of certificates for providing security functions, there is no disclosure, teaching or suggestion in Fischer, as noted by the Final Rejection (page 3, line 26 to page 4, line 2), of providing payment to the certificate authority for processing, i.e., validating, the signed digital message.

To overcome the above deficiencies, the Final Rejection relies on the reference to Kuzma. Kuzma is directed to a method and apparatus for transmitting electronic data using electronic credits to pay for the transmission. In Kuzma, a transmission service provides communications links between a sender and an addressee. The sender uses electronic stamps, previously purchased from the transmission service, to pay for the transmission of the message and the use of the communications links. After preparing an electronic message for sending and selecting an addressee, the file size is examined, for example in bytes, of the data being transmitted and an electronic stamp is attached to the data transmission as payment for the transmission and/or use of the communications channel. The electronic stamp is a data packet that when processed by the carrier or at the addressee location appears as a stamp-like graphic marking on the transmitted document. Substantially concurrently with application of the electronic stamp to the electronic data, a counter or database containing the data corresponding to the sender's amount of electronic stamps is debited in an amount equal to the value of the affixed electronic stamp to reflect the use of the electronic stamp to pay for the electronic transmission of the data or message. (Col. 2, line 53 to Col. 3, line 9). To prevent fraud and theft of services of the carrier, the stamp presented as payment for a transmission can be

authenticated by hiding an authenticating mark in the stamp graphics or by including an authentication data code. (Col. 3, lines 17-44).

Fig. 1 of Kuzma, reproduced below, illustrates a block diagram of a device for transmitting electronic data using attached electronic credits to pay for the transmission.

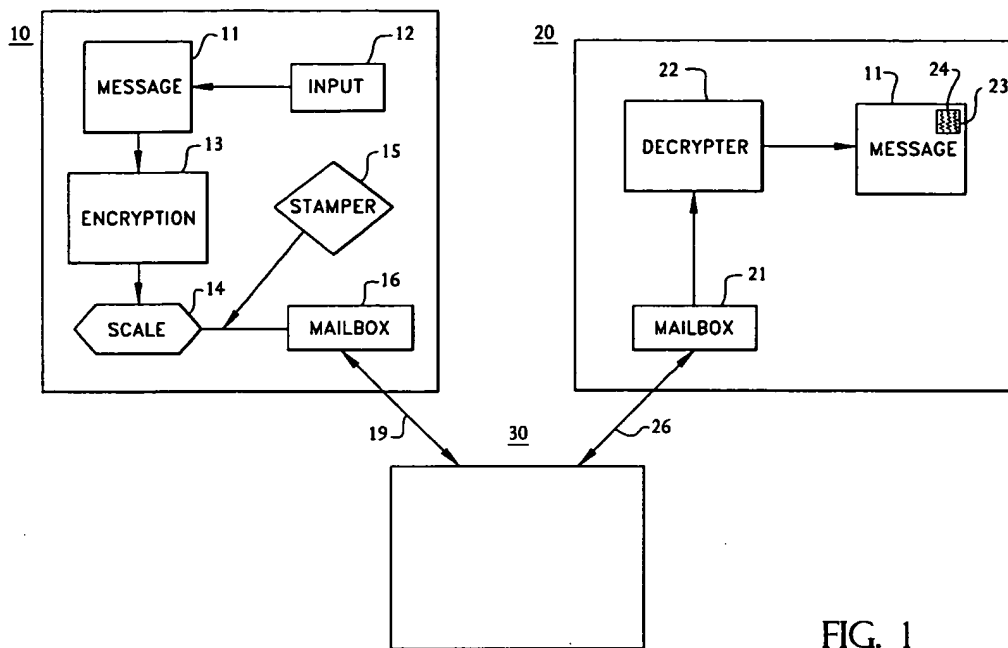


FIG. 1

Electronic message 11, represented by data to be transmitted, is sent from sender terminal 10 for eventual receipt at addressee terminal 20. Sender terminal 10 and addressee terminal 20 preferably are processor controlled. Electronic message 11, input by data input device 12 is then encrypted by encryption device 13. Encryption device 13 simulates placing message 11 into an envelope to obscure the text of the message, thereby rendering it unreadable except at addressee terminal 20. After message 11 has been encrypted, it is "weighed" by scale 14. Scale 14 "weighs" the message to determine the amount of electronic postage required. However, the electronic message cannot be "weighed" in the conventional sense, but instead is examined for file size or number of bytes. After scale 14 measures the amount of electronic postage necessary, stamper 15 affixes an appropriately valued electronic stamp or credit to electronic message 11. Electronic stamp 15 is data recognized by electronic post office 30 as payment for transmission of electronic message 11. After affixation of stamp 15, the stamped, encrypted electronic

message 11 is placed in output mailbox 16, from where it is subsequently transmitted to electronic post office 30 over line 19. Electronic post office 30 transmits electronic message 11 to mailbox 21 at addressee location 20 over line 26. Mailbox 21, especially in the case of computer-based messaging, can be a memory location or the like in which electronic message 11 is stored prior to its opening at addressee location 20. At addressee location 20, the electronic message 11 is decrypted, by decrypter 22, much like a conventional USPS letter is received in an envelope which is opened by the addressee. After decryption, electronic message 11 is displayed in text and/or graphics form from which it can be read/viewed by the addressee. The electronic message 11 displayed at addressee location 20 can include graphics denoting electronic stamp 23. Since electronic stamp 23 has been used to pay for electronic transmission of electronic message 11, electronic stamp 23 bears cancellation marks 24 when viewed at addressee location 20. (Col. 4, line 5 to Col. 5, line 5).

In the Final Rejection, the Examiner agrees that Kuzma does not disclose, teach or suggest a signed digital message or validating a signed digital message. (Office Action, page 2, first paragraph). The top of page 3 of the Office Action, however, states:

Kuzma teaches the use of a register having funds stored therein, determining if sufficient funds are available in the register for validating a message, and deducting funds from the register for validating the message. Thus, Kuzma teaches the concept of using a register having funds stored therein to pay for a service such as validating a message to ensure legitimacy.

As noted above, however, there is no disclosure, teaching or suggestion in Kuzma of a signed digital message or validating a signed digital message. If there is no disclosure, teaching or suggestion in Kuzma of a signed digital message or validating a signed digital message, there can not be any disclosure, teaching or suggestion in Kuzma of using a register having funds stored therein, determining if sufficient funds are available in the register for validating a message, and deducting funds from the register for validating a message. There is no disclosure, teaching or suggestion in either of the cited references, either alone or in combination, of a method for validating a signed digital message that includes "providing a register having funds stored therein; receiving a signed digital message from a sender; determining if sufficient funds

are present in the register for validating the message; deducting funds from the register for validating the message; and validating the signed digital message using a public key of the sender” as is recited in claim 35.

The Final Rejection contends that it would have been obvious to combine the teachings of Fischer and Kuzma, and that by combining the teachings of Kuzma and Fischer one would arrive at the present invention. Appellant respectfully disagrees.

As noted above, Fisher is directed to a public key cryptography system with enhanced digital signature certification that authenticates the identity of the public key holder. Kuzma is directed to a method and apparatus for transmitting electronic data using electronic credits to pay for the transmission. Even if one were motivated to combine the teachings of Fischer and Kuzma, it would simply teach a method and system to pay a transmission service for the electronic transmission of the digital message created and signed by the trusted authority. Transmission of a digital message is not the same as validating a digital message. There is no disclosure, teaching or suggestion in the cited references, either alone or in combination, of a method for validating a signed digital message that includes “providing a register having funds stored therein; receiving a signed digital message from a sender; determining if sufficient funds are present in the register for validating the message; deducting funds from the register for validating the message; and validating the signed digital message using a public key of the sender” as recited in claim 35.

The Final Rejection contends that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to one of ordinary skill in the art. In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). The combination of the teachings of Fischer and Kuzma, however, would simply teach a method and system to pay a transmission service for the electronic transmission of the digital message created and signed by the trusted authority. The fact that the present invention was made by the Appellant does not make the present invention obvious; that suggestion or teaching must come from the prior art. See C.R. Bard, Inc. v. M3 Systems, Inc., 157 F.3d 1340, 1352 (Fed. Cir.

1998). See, e.g., Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051-1052 (Fed. Cir. 1988) (it is impermissible to reconstruct the claimed invention from selected pieces of prior art absent some suggestion, teaching, or motivation in the prior art to do so). The Final Rejection's reconstruction of the present invention from these reference includes knowledge gleaned only from the Appellant's disclosure. Without using the present claims as a road map, it would not have been obvious to make the multiple, selective modifications needed to arrive at the claimed invention from these references. The rejection uses impermissible hindsight to reconstruct the present invention from this reference. See Ex parte Clapp, 227 U.S.P.Q. 972,973 (Bd. App. 1985) (requiring "convincing line of reasoning" to support and obviousness determination).

For at least the above reasons, Appellant respectfully submits that the final rejection as to claim 35 is in error and should be reversed. Claim 36 is dependent upon claim 35 and therefore the final rejection with respect to this claim should also be reversed.

IX. Conclusion

In Conclusion, Appellant respectfully submits that the final rejection of claims 35 and 36 is in error for at least the reasons given above and should, therefore, be reversed.

Respectfully submitted,



Brian A. Lemm
Reg. No. 43,748
Attorney for the Appellant
Telephone (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, Connecticut 06484-8000

APPENDIX A

35. A method for validating a signed digital message, comprising the steps of:
- providing a register having funds stored therein;
 - receiving a signed digital message from a sender;
 - determining if sufficient funds are present in the register for validating the message;
 - deducting funds from the register for validating the message; and
 - validating the signed digital message using a public key of the sender.
36. The method of claim 35, comprising the further steps of:
- receiving with the signed digital message a certificate of the sender, the certificate being signed using a private key of a certificate authority;
 - validating the certificate using a public key of the certificate authority; and
 - extracting the public key of the sender from the certificate for use in validating the signed digital message.